Residue Classes Having Tardy Totients

John B. Friedlander
Department of Mathematics, University of Toronto
Toronto, Ontario M5S 3G3, Canada
frdlndr@math.toronto.edu

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

February 2, 2008

Abstract

We show, in an effective way, that there exists a sequence of congruence classes $a_k \pmod{m_k}$ such that the minimal solution $n = n_k$ of the congruence $\phi(n) \equiv a_k \pmod{m_k}$ exists and satisfies $\log n_k / \log m_k \to \infty$ as $k \to \infty$. Here, $\phi(n)$ is the Euler function. This answers a question raised in [3]. We also show that every congruence class containing an even integer contains infinitely many values of the Carmichael function $\lambda(n)$ and the least such n satisfies $n \ll m^{13}$.

1 Introduction

Let $\phi(n)$ be the Euler function of n. The number $\phi(n)$ is also referred to as the *totient* of n, and so the values of the Euler function are referred to as *totients*. There are a number of papers in the literature dealing with the question of which arithmetical progressions contain infinitely many totients. Since all totients > 1 are even, it follows that the only arithmetical progressions

that can contain infinitely many totients are the ones which contain even integers. Dence and Pomerance [2] established that if a congruence class $a \pmod{m}$ contains at least one multiple of 4, then it contains infinitely many totients. Later, Ford, Konyagin and Pomerance [4] gave a characterization of which arithmetical progressions consisting entirely of numbers congruent to $2 \pmod 4$ contain infinitely many values of the Euler function. They also showed that the union of all such residue classes which are totient-free (i.e., do not contain totients) has asymptotic density $1/4$ (as does the entire progression $2 \pmod 4$), establishing in this way that almost all integers which are $\equiv 2 \pmod 4$ are in a residue class that is totient-free. See also [9] for related results.

Recently, the first–named author and Shparlinski [3] looked at progressions $a \pmod{m}$ containing totients and asked about the size of the smallest totient, denoted by $N(a, m)$, in such a progression. Under the restriction $\gcd(2a, m) = 1$ (note that in this case m is necessarily odd), they established that $N(a, m) \le m^{3+o(1)}$ holds uniformly in a and m as $m \to \infty$. When m is prime, the exponent 3 can be improved to 2.5. They asked whether a similar result holds, perhaps with an exponent larger than 3, provided that one eliminates the assumption that $2a$ and m are coprime. Specifically, Open Question 7 in [3] is the following.

Open Question. *Does there exist a positive constant A such that, for every pair of integers a and m, if there exists an integer n with $\phi(n) \equiv a \pmod{m}$, then there exists such an integer with $n < m^A$?*

Here, we give a negative answer to the above question. In what follows, we write $\log x$ for the natural logarithm of x. Our result is the following.

Theorem 1. *There exists a sequence $a_k \pmod{m_k}$ of arithmetical progressions with $m_k \to \infty$ such that $N(a_k, m_k)$ exists and satisfies*

$$N(a_k, m_k) \ge m_k^{(c_0+o(1))(\log\log m_k/\log\log\log m_k)^{1/2}} \tag{1}$$

as $k \to \infty$, where $c_0 > 0$ is an absolute constant.

The value $c_0 = 2/5$ is acceptable in Theorem 1. Under the hypothesis of the Generalized Riemann Hypothesis for certain algebraic number fields our argument yields the stronger lower bound

$$N(a_k, m_k) \ge m_k^{(c_1+o(1))(\log m_k/\log\log m_k)^{1/2}}\ , \tag{2}$$

as $k \to \infty$, where $c_1 = 2^{-1/2}$.

While the Euler function $\phi(n)$ measures the size of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, the exponent of this group (i.e., largest order of elements) is called the *Carmichael function* of n and is denoted by $\lambda(n)$. Since $(-1)^2 \equiv 1 \pmod n$, it follows that $\lambda(n)$ is even for all $n \geq 3$. While the existence of totients in arithmetical progressions has received interest, the analogous problem concerning the presence of values of the Carmichael function in residue classes seems not to have been investigated. Although it is often the case that problems for the latter function are the more difficult of the two, in case of the question of which progressions occur, the Carmichael function is the easier. As for the question answered for ϕ by Theorem 1, the answer for λ is the opposite.

Theorem 2. *If the arithmetical progression $a \pmod m$ contains an even number, then it contains infinitely many values of the Carmichael function. Furthermore, writing $L(a,m)$ for the least integer n such that $\lambda(n) \equiv a \pmod m$, we have $L(a,m) \ll m^{13}$.*

2 Proof of Theorem 1

We start with the following lemma.

Lemma 1. *Let $k \geq 2$ be an integer and $a = 2q$, where $q > 3$ is prime. Then $f_k(X) = X^k - X^{k-1} - a \in \mathbb{Q}[X]$ is irreducible.*

Proof. Assume for a contradiction that $f_k(X) = g(X)h(X)$, where $g(X)$ and $h(X)$ are monic, with integer coefficients and positive degrees. Reducing modulo q, we get $g(X)h(X) \equiv X^{k-1}(X-1) \pmod q$, therefore, up to relabeling the polynomials $g(X)$ and $h(X)$, we may assume that $g(X) = X^\alpha(X-1) \pmod q$ and $h(X) = X^\beta \pmod q$, where $\alpha + \beta = k$. If $\alpha\beta > 0$, then $g(0) \equiv h(0) \equiv 0 \pmod q$. Thus, the last coefficient of each of $g(X)$ and $h(X)$ is a multiple of q. This implies that the last coefficient of $f_k(X)$, which is $f_k(0) = -a = -2q = g(0)h(0)$ is a multiple of q^2, which is a contradiction. This shows that $\alpha\beta = 0$ and since both $g(X)$ and $h(X)$ have positive degrees, it follows that $\alpha = 0$. Hence, $g(X) \equiv X - 1 \pmod q$, therefore $g(X)$ is linear. Write $g(X) = X - x_0$ for some $x_0 \in \mathbb{Z}$ with $x_0 \equiv 1 \pmod q$. Then x_0 is a root of $f_k(X)$, therefore $2q = a = x_0^{k-1}(x_0 - 1)$. Since $q \mid x_0 - 1$, it follows that $x_0^{k-1} \mid 2$. If $k \geq 3$, we get $x_0 = \pm 1$, therefore

$2q = x_0^{k-1}(x_0 - 1) \in \{0, \pm 2\}$, which is impossible. If $k = 2$, we then get that $x_0 \in \{\pm 1, \pm 2\}$, therefore $2q = a = x_0(x_0 - 1) \in \{0, 2, 6\}$, which is again impossible. Hence, $f_k(X) \in \mathbb{Q}[X]$ is irreducible. $\square$

We are now ready to prove Theorem 1. Let L be any large even integer. We let $q > L$ be a prime congruent to 1 modulo 3, put $a = 2q$ and let again $f_k(X) = X^k - X^{k-1} - a \in \mathbb{Q}[X]$ be the polynomials that appear in Lemma 1 for $k = 2, 3, \ldots, L$. They are all irreducible by Lemma 1. For each $k = 2, \ldots, L$, we let θ_k be some root of $f_k(X)$. We write $\theta_k^{(1)}, \ldots, \theta_k^{(k)}$ for all the conjugates of θ_k with the convention that $\theta_k^{(1)} = \theta_k$. We put $\mathbb{K}_k^{(j)} = \mathbb{Q}[\theta_k^{(j)}]$ for $j = 1, \ldots, k$. We also put $\overline{\mathbb{K}_k} = \mathbb{Q}[\theta_k^{(1)}, \ldots, \theta_k^{(k)}]$ for the splitting field of $f_k(X)$ and $\mathbb{M} = \mathbb{Q}[\theta_k^{(j)} : 2 \le k \le L, 1 \le j \le k]$ for the splitting field of $\prod_{k=2}^{L} f_k(X)$. Our first objective is to insure that we can choose an appropriate a of the desired form which is not too large such that $G = \mathrm{Gal}(\mathbb{M}/\mathbb{Q}) = \prod_{k=2}^{L} S_k$, where we write S_m for the symmetric group on m letters.

We start by computing the discriminant of $\mathbb{K}_k = \mathbb{K}_k^{(1)}$. It is well-known (see [11]) that if $f(X) = X^n + AX^s + B \in \mathbb{Q}[X]$, where $1 \le s \le n-1$, then the discriminant of the polynomial $f(X)$ is

$$\Delta(f) = (-1)^{n(n-1)/2} B^{s-1} \left(n^n B^{n-s} + (-1)^{n-1} s^s (n-s)^{n-s} A^n \right).$$

Thus, if we put $\Delta_k = \Delta(f_k)$, we then have that $n = k,\ s = k-1,\ A = -1$ and $B = -a$, therefore

$$\Delta_k = (-1)^{(k-1)(k+2)/2} a^{k-2} (a k^k + (k-1)^{k-1}).$$

Let $\mathcal{M}$ be the set of all prime numbers $p \ne 2,\ q$ that can appear as divisors of $\gcd(\Delta_j, \Delta_k)$ for some $2 \le j < k \le L$. If $p \ne 2, q$ is a prime factor of Δ_j, then $p \mid a j^j + (j-1)^{j-1}$. Since j and $j-1$ are coprime, we see that $p \nmid j$, therefore j is invertible modulo p. Thus, $a \equiv -(j-1)^{j-1} j^{-j} \pmod{p}$. If additionally $p \mid \Delta_k$, then also $a \equiv -(k-1)^{k-1} k^{-k} \pmod{p}$. Thus,

$$-(j-1)^{j-1} j^{-j} \equiv -(k-1)^{k-1} k^{-k} \pmod{p}$$

leading to $p \mid (j-1)^{j-1} k^k - j^j (k-1)^{k-1}$. Thus, writing

$$M = \prod_{2 \le j < k \le L} \left((j-1)^{j-1} k^k - j^j (k-1)^{k-1} \right),$$

we conclude that

$$\prod_{p\in\mathcal{M}} p \mid M.$$

Note that $M > 0$ since the function $x \mapsto (x-1)^{x-1}x^{-x}$ is decreasing for $x \ge 2$. Note further that M consists of a product of $\binom{L-1}{2}$ factors none of which exceeds $L^L(L-1)^{L-1} < L^{2L}$. Thus,

$$M \le \left(L^{2L}\right)^{\binom{L-1}{2}} < L^{L^3}.$$

Thus, writing $\omega(m)$ for the number of distinct prime factors of m and using the known fact that $\omega(m) \le (1+o(1))\log m/\log\log m$ as $m \to \infty$, we get that

$$\begin{aligned}\#\mathcal{M} &\le \omega(M) \le (1+o(1))\frac{\log M}{\log\log M} \le (1+o(1))\frac{L^3\log L}{\log(L^3\log L)}\\ &\le (1/3+o(1))L^3 \end{aligned} \tag{3}$$

as $L \to \infty$.

Let $T > L$ be some large number to be determined later. We search for a value of $a = 2q$, where $L < q \le T$ is prime congruent to 1 modulo 3, such that for each $k = 2,\dots,L$ there exists a prime $p_k \| \Delta_k$ such that p_k does not divide any of the Δ_j for $j \ne k$ in $\{2,\dots,L\}$. To conclude that such a q exists, assume the contrary. Then for each prime $q \in (L,T]$ congruent to 1 modulo 3, there exists $k \in \{2,\dots,L\}$ such that $ak^k + (k-1)^{k-1} = sy$ holds with some square-free number s dividing $2M$ and some positive integer y which is square-full. Recall that a positive integer m is square-full if $p^2 \mid m$ whenever p is a prime factor of m. The number of choices for s is at most $2^{\omega(M)+1}$. For a large positive real number x, the number of square-full numbers $y \le x$ does not exceed $3x^{1/2}$ (see, for example, Théorème 14.4 in [6]). Since $ak^k + (k-1)^{k-1} \le 2aL^L \le 4TL^L$, it follows that y can be chosen in at most $3(4TL^L)^{1/2}$ ways. Hence, the number of possibilities for $a \in (L,T]$ such that there exists $k \in \{2,\dots,L\}$ with $ak^k+(k-1)^{k-1} = sy$, where $s \mid 2M$ and y is square-full is

$$\le 3(L-1)2^{\omega(M)+1}(4TL^L)^{1/2}.$$

Since there are $\pi(T;3,1) - \pi(L;3,1)$ primes $q \in (L,T]$, we get that a desired choice for a is possible once

$$\pi(T;3,1) - \pi(L;3,1) > 3(L-1)2^{\omega(M)+1}(4TL^L)^{1/2}. \tag{4}$$

Here, we used, as usual, for coprime integers a and b the notation $\pi(x;b,a)$ for the number of primes $p \le x$ congruent to a modulo b. Let T_L be the minimal positive integer satisfying inequality (4). Estimate (3) together with standard estimates for primes in arithmetical progressions shows that

$$T_L \le \exp((2(\log 2)/3 + o(1))L^3) \qquad \text{as } L \to \infty.$$

Since $p_k \neq 2, q$ exactly divides Δ_k, it follows that $p_k \mid \Delta_{\mathbb{K}_k}$, where for a field $\mathbb{L}$ we put $\Delta_{\mathbb{L}}$ for its discriminant. Furthermore, Theorem 1.1 in [1] and the remarks following it show that if $f(X) = X^n + AX^s + B$ is irreducible, with integer coefficients and satisfies the conditions $\gcd(n, As) = \gcd(A(n-s), B) = 1$ and there is a prime divisor q of B such that $q \| b$, then the Galois group $G(f)$ of $f(X)$ over $\mathbb{Q}$ is doubly transitive. When $f(X) = f_k(X)$, we have that $n = k,\ s = k-1, A = -1$ and $B = -a = -2q$, therefore all three conditions $\gcd(n, As) = \gcd(A(n-s), B) = 1$ and $q \| B$ are satisfied. Thus, the Galois group of $f_k(X)$ over $\mathbb{Q}$ is doubly transitive. The remarks following Theorem 1.1 in [1] show that if furthermore there exists a prime p_k not dividing $\gcd(k-1, 2q)$ (which for us equals 1 or 2 since $q > L$) such that p_k exactly divides Δ_k, then the Galois group of $f_k(X)$ over $\mathbb{Q}$ contains a transposition and is, in particular, the full symmetric group S_k. Thus, we have showed that $\mathrm{Gal}(\mathbb{K}_k/\mathbb{Q}) = S_k$.

We are now ready to show that $G = \prod_{k=2}^{L} S_k$. Since $\mathrm{Gal}(\mathbb{K}_k/\mathbb{Q}) = S_k$ for each $k \in \{2, \ldots, L\}$, it suffices to show the family of fields $\{\overline{\mathbb{K}_k} : k = 2, \ldots .L\}$ consists of *linearly disjoint* fields, namely that if $\{k_1, \ldots, k_{s+1}\}$ is any subset of $\{2, \ldots, L\}$ with $k_{s+1} \notin \{k_1, \ldots, k_s\}$, then

$$\overline{\mathbb{K}_{k_1}\mathbb{K}_{k_2}} \cdots \overline{\mathbb{K}_{k_s}} \cap \overline{\mathbb{K}_{k_{s+1}}} = \mathbb{Q}. \tag{5}$$

Well, let us denote by $\mathbb{L}$ the field appearing in the left hand side of the above equality and assume that it is not $\mathbb{Q}$. Since $\mathbb{L}$ is an intersection of normal extensions of $\mathbb{Q}$, it follows that it is itself a normal extension of $\mathbb{Q}$. Furthermore, if p is a prime dividing $\Delta_{\mathbb{L}}$ then p divides both $\Delta_{k_{s+1}}$ and $\prod_{i=1}^{s} \Delta_{k_i}$. In particular, $p \neq p_{k_{s+1}}$, which shows that $\mathbb{L} \not\subseteq \overline{\mathbb{K}_{k_{s+1}}}$. Since $\mathbb{L}$ is a normal extension of $\mathbb{Q}$ properly contained in $\overline{\mathbb{K}_{k_{s+1}}}$, it follows that $\mathrm{Gal}(\mathbb{K}_{k_{s+1}}/\mathbb{L})$ is a normal proper subgroup of $\mathrm{Gal}(\mathbb{K}_{k_{s+1}}/\mathbb{Q}) = S_k$. The only such subgroup is A_k and, by Galois correspondence, we get that $\mathbb{L} = \mathbb{Q}(\sqrt{\Delta_{\mathbb{K}_{k_{s+1}}}})$. But this last quadratic field has the property that $p_{k_{s+1}}$ divides its discriminant,

whereas we have established that the prime $p_{k_{s+1}}$ cannot divide the discriminant of the field $\mathbb{L}$. This contradiction shows that indeed equality (5) holds, which establishes our claim on the structure of the Galois group of $\mathbb{M}$.

Let $\mathcal{C}$ be a conjugacy class of G containing an element $\sigma = (\sigma_2, \ldots, \sigma_L)$ where $\sigma_k \in S_k$ has no fixed points for all $k = 2, \ldots, L-1$, but $\sigma_L \in S_L$ is the identical permutation. By Chebotarev's Density Theorem, a positive proportion of all the primes p not dividing the discriminant of $\mathbb{M}$ have the property that their Frobenius Frob_p is in the conjugacy class $\mathcal{C}$. If p is such a prime, then $f_k(X) \pmod p$ has no root modulo p for any $k = 2, \ldots, L-1$, while $f_L(X) \pmod p$ splits in linear factors modulo p.

We now let x be a large positive real number. We need a lower bound for the number of primes $p \le x$ in the conjugacy class $\mathcal{C}$ of G. To this end, we use the following result which is implicit in the work of Lagarias, Montgomery and Odlyzko on the least prime ideal in the Chebotarev Density Theorem [8].

Lemma 2. *Let $\mathbb{M}$ be a Galois extension of $\mathbb{Q}$ of discriminant $\Delta_{\mathbb{M}}$ having Galois group G. Let $\mathcal{C}$ be a conjugacy class in G and define*

$$\pi_{\mathcal{C}}(x, \mathbb{M}/\mathbb{Q}) = \#\{p \le x : p \nmid \Delta_{\mathbb{M}},\ \mathrm{Frob}_p \in \mathcal{C}\}.$$

There exist absolute constants A_1 and A_2 such that if $x > |\Delta_{\mathbb{M}}|^{A_1}$, then

$$\pi_{\mathcal{C}}(x, \mathbb{M}/\mathbb{Q}) \gg \frac{\#\mathcal{C}}{\#G} \frac{x^{1/5}}{|\Delta_{\mathbb{M}}|^{A_2}}. \tag{6}$$

Proof. Let

$$\mathcal{P}(\mathcal{C}) = \{p \ :\ p \nmid \Delta_{\mathbb{M}},\ \mathrm{Frob}_p \in \mathcal{C}\}.$$

Inequality (6.9) in [8] shows that there exist positive absolute constants B_1, B_2, B_3 and B_4 such that

$$\begin{aligned} \sum_{\substack{p \in \mathcal{P}(\mathcal{C}) \\ p \le x^{10}}} (\log p) \widehat{k_2}(p) \quad &\ge \quad \frac{x^2}{10} \frac{\#\mathcal{C}}{\#G} \min\{1, (1-\beta_0)\log x\} - B_1 x^{7/4} \log |\Delta_{\mathbb{M}}| \\ &- \quad B_2 x^2 (1-\beta_0)^{B_3 \log x / \log |\Delta_{\mathbb{M}}|} \log |\Delta_{\mathbb{M}}|, \end{aligned} \tag{7}$$

where $\beta_0 \in (0,1)$ satisfies $1 - \beta_0 > |\Delta_{\mathbb{M}}|^{-B_4}$ (see Corollary 5.2 on page 290 in [8]), and $\widehat{k_2}(u)$ is a function whose range is in the interval $(0,1)$ (see formula

(3.7) on page 284). The argument on the top of page 294 in [8], shows that if we choose $x > |\Delta_{\mathbb{M}}|^{B_5}$ for a suitable absolute constant $B_5 > 0$, then the first term in the right hand side of inequality (7) dominates. Thus, inequality (7) implies that

$$\pi_{\mathcal{C}}(x^{10}, \mathbb{M}/\mathbb{Q}) \log x \gg \frac{\#\mathcal{C}}{\#G} x^2 \min\{1, (1-\beta_0)\log x\} \gg \frac{\#\mathcal{C}}{\#G} \frac{x^2 \log x}{|\Delta_{\mathbb{M}}|^{B_4}},$$

which in turn implies that

$$\pi_{\mathcal{C}}(x^{10}, \mathbb{M}/\mathbb{Q}) \gg \frac{\#\mathcal{C}}{\#G} \frac{x^2}{|\Delta_{\mathbb{M}}|^{B_4}},$$

which is what we wanted to prove with $A_1 = 10B_5$ and $A_2 = B_4$. $\square$

For an algebraic number field $\mathbb{L}$, we write $d_{\mathbb{L}}$ for its degree. In order to apply the above Lemma 2, we need upper bounds on $\Delta_{\mathbb{M}}$. Clearly,

$$\begin{aligned} d_{\mathbb{M}} &= \#G = \prod_{k=2}^{L} k! \le \prod_{k=2}^{L} k^k = \exp\left(\sum_{k=2}^{L} k \log k\right) \\ &= \exp\left((1/2 + o(1))L^2 \log L\right), \qquad \text{as } L \to \infty. \end{aligned} \tag{8}$$

As for $|\Delta_{\mathbb{M}}|$, we use recursively the fact that if $\mathbb{K} \cap \mathbb{L} = \mathbb{Q}$, then

$$|\Delta_{\mathbb{KL}}|^{1/d_{\mathbb{KL}}} \le |\Delta_{\mathbb{K}}|^{1/d_{\mathbb{K}}} |\Delta_{\mathbb{L}}|^{1/d_{\mathbb{L}}} \tag{9}$$

(see, for example, Proposition 4.9 of [10]). Note first that since the inequality

$$|\Delta_{\mathbb{K}_k}| = a^{k-2}(ak^k + (k-1)^{k-1}) < T_L^k$$

holds for all sufficiently large L, it follows that $|\Delta_{\mathbb{K}_k}|^{1/k} \le T_L$. Since $\overline{\mathbb{K}_k}$ is the compositum of the k linearly disjoint fields ${\mathbb{K}_k}^{(j)}$ each of degree k for $j = 1, \ldots, k$ all having the property that $|\Delta_{\mathbb{K}_k^{(j)}}|^{1/k} \le T_L$, repeated applications of inequality (9) give $|\Delta_{\overline{\mathbb{K}_k}}|^{1/k!} \le T_L^k$. Finally, since $\mathbb{M}$ is the compositum of the linearly disjoint fields $\overline{\mathbb{K}_k}$ for $k = 2, \ldots, L$ of degrees $k!$, respectively, repeated applications of inequality (9) once more give that

$$\begin{aligned} |\Delta_{\mathbb{M}}|^{1/d_{\mathbb{M}}} &\le \prod_{k=2}^{L} |\Delta_{\overline{\mathbb{K}_k}}|^{1/k!} \le \prod_{k=2}^{L} T_L^k < T_L^{L(L+1)/2} \\ &= \exp(((\log 2)/3 + o(1))L^5), \qquad \text{as } L \to \infty. \end{aligned} \tag{10}$$

In particular, the inequality

$$|\Delta_{\mathbb{M}}| \le \exp\left(d_{\mathbb{M}} L^5\right) \tag{11}$$

holds once L is sufficiently large. Assume now that $\varepsilon \in (0, 1/20)$, and that

$$(1/2+\varepsilon)L^2 \log L < \log\log x. \tag{12}$$

We then get that if $x > x_\varepsilon$, then

$$d_{\mathbb{M}} L^5 < \frac{\log x}{\log\log x},$$

which in turn implies, via inequality (11), that

$$x > |\Delta_{\mathbb{M}}|^{\log\log x}.$$

Hence, inequality (6) together with the fact that $\#G \le d_{\mathbb{M}} \ll \log|\Delta_{\mathbb{M}}|$, gives that

$$\pi_{\mathcal{C}}(x, \mathbb{M}/\mathbb{Q}) \ge x^{1/5-\varepsilon}. \tag{13}$$

So, we see from (12) that if we take

$$L = \lfloor (2-\varepsilon/3)(\log\log x/\log\log\log x)^{1/2} \rfloor - \delta,$$

where $\delta \in \{0, 1\}$ is chosen in such a way so that L is even, then inequality (12) (and hence, inequality (13) also) is satisfied when x is sufficiently large.

We now discard the subset $\mathcal{Q}$ of primes $p \le x$ such that $p \mid r^M - r^{M-1} - a$ for some prime $r \le x^{1/5-2\varepsilon}$ and some $M \in [L, 2L\log x]$. Fixing r and M, the number of such primes is $\le \omega(|r^M - r^{M-1} - a|)$ (note that the integer $r^M - r^{M-1} - a$ is not zero since $f_M(X) \in \mathbb{Q}[X]$ is irreducible for all $M \ge 2$). Thus, the number of such choices is

$$< \max\{\log(r^M), \log a\} < \max\{M \log x, \log T_L\} < 2L(\log x)^2$$

once x is large. Summing this up over all the $\pi(x^{1/5-2\varepsilon})$ choices of the prime $r \le x$ and over all the $\lfloor 2L\log x \rfloor - L + 1$ choices for M, we have that

$$\#\mathcal{Q} < 4\pi(x^{1/5-2\varepsilon})L^2(\log x)^3 < 200x^{1/5-2\varepsilon}(\log x)^2(\log\log x)^2$$

possibilities for p once x is large. Thus, if $x > x_\varepsilon$, then

$$\pi_{\mathcal{C}}(x, \mathbb{M}/\mathbb{Q}) - \#\mathcal{Q} \ge x^{1/5-\varepsilon} - 200x^{1/5-2\varepsilon}(\log x)^2(\log\log x)^2 > x^{1/5-2\varepsilon},$$

so in particular there are such primes $p > x^{1/5-2\varepsilon}$ which are not in $\mathcal{Q}$.

Let p be one such prime. Look at congruence $a \pmod{m}$, where $m = 12p$. Assume that $\phi(n) \equiv a \pmod{m}$. Since $2\|a$ and m is a multiple of 4, it follows that either $n = 4$ or $n = r^\ell$ or $2r^\ell$ for some odd prime r and positive integer ℓ. If $n = 4$, we get $2 \equiv a \pmod{p}$, therefore $p \mid 2(q-1)$, which is impossible since

$$2(q-1) \le a \le T_L = \exp(O(\log\log x)^3) = x^{o(1)}$$

as $x \to \infty$, while $p \ge x^{1/5-2\varepsilon}$. Thus, $n = r^\ell$ or $2r^\ell$, therefore $\phi(n) = r^\ell - r^{\ell-1}$. Hence, $r^\ell - r^{\ell-1} - a \equiv 0 \pmod{m}$. If $\ell = 1$, we get that $r \equiv a+1 \pmod{m}$. Since $a + 1 = 2q + 1 \equiv 0 \pmod{3}$ and $3 \mid m$, it follows that $3 \mid r$, and since r is prime we get that $r = 3$. Thus, $m \mid a - 2$, leading again to $p \mid 2(q-1)$, which is impossible. Thus, $\ell \ge 2$. Since $r^\ell - r^{\ell-1} - a \equiv 0 \pmod{p}$ with some $\ell \ge 2$, it follows, from the way p was chosen, that $\ell \ge L$ because $f_k(X) \pmod{p}$ has no root modulo p for any $k = 2, \ldots, L-1$. Thus, $\ell \ge L$. Since also $p \notin \mathcal{Q}$, we get that either $\ell \ge 2L\log x$, therefore

$$n \ge r^\ell \ge 2^{2L\log x} = x^{(2\log 2)L} > m^L$$

for large x, or $\ell \in [L, 2L\log x]$, in which case $r > x^{1/5-2\varepsilon}$, therefore

$$r^\ell \ge x^{(1/5-2\varepsilon)L} > m^{(1/5-3\varepsilon)L}$$

once x is sufficiently large. Since $\varepsilon > 0$ is arbitrary, this shows that the smallest n such that $\phi(n) \equiv a \pmod{m}$ satisfies indeed inequality (1) as $m \to \infty$, provided that it exists.

It remains to show that the progression $a \pmod{m}$ contains totients. Well, from the way we choose p, the equation $X^L - X^{L-1} \equiv a \pmod{p}$ has a solution modulo p (in fact, L distinct ones). Since p and a are coprime, it follows that any solution $X \equiv x_0 \pmod{p}$ of the above congruence has the property that x_0 is not a multiple of p. Let r be a prime such that $r \equiv x_0 \pmod{p}$. Then, $r^L - r^{L-1} - a$ is a multiple of p. Imposing also that $r \equiv 3 \pmod{4}$, we get that $r^L - r^{L-1} - a = r^{L-1}(r-1) - 2q$ is also a multiple of 4. Finally, choosing $r \equiv 2 \pmod{3}$, since L is even, we get $r^L - r^{L-1} - a \equiv 1 - 2 - 2q \equiv 0 \pmod{3}$, because $q \equiv 1 \pmod{3}$. Thus, it is enough to choose primes r such that $r \equiv x_0 \pmod{p}$, $r \equiv 3 \pmod{4}$ and $r \equiv 2 \pmod{3}$. The above system of congruences is solvable by the Chinese Remainder Lemma and its solution is a congruence class modulo $m = 12p$ which is coprime to m. This class contains infinitely many primes

r by Dirichlet's theorem on primes in arithmetical progressions and if r is any such prime then putting $n = r^L$ we have that the totient $\phi(n)$ is indeed congruent to $a \pmod m$.

This completes the proof of Theorem 1. $\square$

Remark. Under the Generalized Riemann Hypothesis for the fields $\mathbb{M}$ constructed in the previous proof, we have

$$\left|\pi_{\mathcal{C}}(x, \mathbb{M}/\mathbb{Q}) - \frac{\#\mathcal{C}}{\#G}\mathrm{li}(x)\right| \ll \frac{\#\mathcal{C}}{\#G} x^{1/2} \log(|\Delta_{\mathbb{M}}| x^{d_{\mathbb{M}}}) + \log|\Delta_{\mathbb{M}}| \tag{14}$$

(see [7]). With our bound (10), we have

$$\log(|\Delta_{\mathbb{M}}| x^{d_{\mathbb{M}}}) \ll d_{\mathbb{M}}(L^5 + \log x).$$

Inequality (8) shows that if $\varepsilon \in (0, 1/2)$ and the inequality

$$(1/2 + \varepsilon)L^2 \log L < (\log x)/2,$$

holds, then estimate (14) leads to

$$\pi_{\mathcal{C}}(x, \mathbb{M}/\mathbb{Q}) \ge \frac{\pi(x)}{2\#G} \ge x^{1/2 - 10\varepsilon}$$

provided that $x > x_\varepsilon$. We apply again our previous argument except that the set $\mathcal{Q}$ is now taken to be the set of all primes p that divide $r^M - r^{M-1} - a$ for some $M \in [L, 2L \log x]$ and some prime $r \le x^{1/2 - 20\varepsilon}$ and conclude that there exist primes $p > x^{1/2 - 10\varepsilon}$ which are not in $\mathcal{Q}$. Using again the fact that $\varepsilon \in (0, 1/2)$ can be chosen to be arbitrarily small, our previous arguments now easily lead to the conclusion that the better inequality (2) holds in this case with $c_1 = 2^{-1/2}$. We give no further details.

3 Proof of Theorem 2

If $a = 0$, we take n to be the first prime in the arithmetical progression $1 \pmod m$. By Heath-Brown's work on the Linnik constant [5] we know that $n \ll m^{5.5}$. Clearly, $\lambda(n) = n - 1 \equiv 0 \pmod m$. From now on, we assume that $1 \le a \le m - 1$. If m is odd, we replace m by $2m$ and a by the even number among a and $a + m$ (note that since m is odd, it follows that a and

$a+m$ have different parities). Let $a = 2^\alpha a_0$, where $\alpha \geq 0$ and a_0 is odd. We replace m by $M = 2^\alpha m$. Writing $\nu_2(k)$ for the exponent of 2 in the factorization of k, we have that $1 \leq \nu_2(k) < \nu_2(M)$. Let $d = \gcd(a, M)$. Note that $2^\alpha \mid d$ and that $d/2^\alpha \mid m$. Put $a_1 = a/d,\ m_1 = M/d$ and note that d is even, a_1 is odd and m_1 is even. We now search for $n = p_1 p_2$, where $p_1,\ p_2$ are primes of the form $p_1 = d\lambda_1 + 1,\ p_2 = d\lambda_2 + 1$ and $\gcd(p_1 - 1, p_2 - 1) = d$. In this case, $\lambda(n) = d\lambda_1\lambda_2$, and now the congruence $\lambda(n) \equiv a \pmod{M}$ is equivalent to

$$\lambda_1\lambda_2 \equiv a_1 \pmod{m_1}. \tag{15}$$

Since p_1 and p_2 need to be prime numbers, by Dirichlet's theorem on primes in arithmetical progressions, it suffices for their existence that aside from the congruence (15), the conditions $\gcd(d\lambda_1 + 1, m_1) = \gcd(d\lambda_2 + 1, m_1) = 1$ are also fulfilled.

We consider three different possibilities for the prime divisors of m_1. First let $p \mid d$ and assume that $p^\beta \| m_1$ for some $\beta \geq 1$. In this case the conditions $\gcd(d\lambda_1 + 1, m_1) = \gcd(d\lambda_2 + 1, m_1) = 1$ are automatically satisfied for any choices. Moreover, since p does not divide a_1, we can choose $\lambda_1 \equiv a_1 \pmod{p^\beta}$ and $\lambda_2 \equiv 1 \pmod{p^\beta}$. Note that $p = 2$ is such a prime.

Assume next that $p \nmid d$ and let $p^\beta \| m_1$ again for some $\beta \geq 1$. Note that both a_1 and d are invertible modulo p and that p is odd. If $a_1 d^2 \not\equiv -1 \pmod{p}$, then we choose $\lambda_1 \equiv a_1 d \pmod{p^\beta}$ and $\lambda_2 \equiv d^{-1} \pmod{p^\beta}$. Then certainly $\lambda_1\lambda_2 \equiv a_1 \pmod{p^\beta}$. Furthermore, $\lambda_1 d + 1 \equiv a_1 d^2 + 1 \not\equiv 0 \pmod{p}$, therefore p does not divide $\lambda_1 d + 1$. Similarly, $\lambda_2 d + 1 \equiv 2 \not\equiv 0 \pmod{p}$, because p is odd, so $\lambda_2 d + 1$ is coprime to p.

Finally, assume that $a_1 d^2 \equiv -1 \pmod{p}$. Let ρ_p be some primitive root modulo p^β, which exists since p is odd, and take $\lambda_1 \equiv \rho_p d^{-1} \pmod{p^\beta}$, and $\lambda_2 = a_1 d \rho_p^{-1} \pmod{p^\beta}$. Clearly, $\lambda_1\lambda_2 \equiv a_1 \pmod{p^\beta}$. Furthermore, $\lambda_1 d + 1 \equiv \rho_p + 1 \not\equiv 0 \pmod{p}$, because -1 is not a primitive root modulo p. Similarly, $\lambda_2 d + 1 \equiv a_1 d^2 \rho_p^{-1} + 1 \equiv -\rho_p^{-1} + 1 \pmod{p}$, and this last congruence class is not zero since 1 is not a primitive root modulo p.

Hence, for all prime powers p^β dividing m_1 we have constructed congruence classes λ_1 and λ_2 modulo p^β such that the congruence (15) holds modulo p^β and $\lambda_1 d + 1,\ \lambda_2 d + 1$ are not multiples of p. By Dirichlet's theorem on primes in arithmetical progressions, we can choose two distinct primes p_1 and p_2 such that if we put $n = p_1 p_2$, then indeed $\lambda(n) \equiv a \pmod{m}$. Furthermore, by Heath-Brown's result mentioned earlier, we can choose both λ_1 and

λ_2 such that $\max\{\lambda_1, \lambda_2\} \ll m_1^{5.5}$. This shows that

$$\max\{p_1, p_2\} \ll m_1^{5.5} d \ll \left(\frac{2^\alpha m}{d}\right)^{5.5} d \ll 2^\alpha m^{5.5} \left(\frac{2^\alpha}{d}\right)^{4.5} \ll m^{6.5},$$

leading to $n = p_1 p_2 \ll m^{13}$.

References

[1] S. D. Cohen, A. Movahhedi and A. Salinier, 'Double transitivity of Galois groups of trinomials', *Acta Arith.* **82** (1997), 1–15.

[2] T. Dence and C. Pomerance, 'Euler's function in residue classes', *The Ramanujan J.* **2** (1998), 7–20.

[3] J. B. Friedlander and I. E. Shparlinski, 'Least totient in a residue class', *Bull. Lond. Math. Soc.* **39** (2007), 425–432.

[4] K. Ford, S. Konyagin and C. Pomerance, 'Residue classes free of values of the Euler function', in *Number Theory in Progress*, K. Győry, H. Iwaniec, and J. Urbanowicz, eds., vol. 2, de Gruyter, Berlin and New York, 1999, 805-812.

[5] D. R. Heath-Brown, 'Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression', *Proc. London Math. Soc.* **64** (1992), 265–338.

[6] A. Ivić, *The Riemann Zeta-Function, Theory and Applications*, Dover Publications, Minneola, New York, 2003.

[7] J. C. Lagarias and A. M. Odlyzko, 'Effective versions of the Chebotarev Density Theorem', in *Algebraic Number Fields*, Academic Press, New York, 1977, 409–464.

[8] J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko, 'A bound for the least prime ideal in the Chebotarev Density Theorem', in *Invent. Math.*, **54**, (1979), 271–296.

[9] W. Narkiewicz, 'Uniform distribution of sequences of integers in residue classes', in Lecture Notes in Math., vol. **1087**, Springer-Verlag, Berlin, 1984.

[10] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer-Verlag, Berlin, 1990.

[11] R. G. Swan, 'Factorization of polynomials over finite fields', *Pacific J. Math.* **12** (1962), 1099–1106.